REMARKS

NEW CLAIMS

Applicant presents, for the Examiner's consideration, new dependent claims 94-99. These claims find support throughout the specification, and in particular, between column 9, line 34 and column 10, line 20.

IDS

The Office Action indicates that four initialed PTO-1449 forms are to have accompanied it. However, Applicant has not received these initialed forms.

PRIORITY CLAIM

Applicant draws attention to the transmittal letter for this application, and in particular to paragraph 5(b) on page 2. The text of the transmittal letter carries out the necessary amendment.

SECTION 102 REJECTION OF CLAIMS 55 AND 93

Applicant cancels claims 55 and 93 in an effort to expedite prosecution of the remaining claims. Cancellation of these claims is not intended to be an admission that Applicant considers them unpatentable in view of the cited art. Applicant reserves the right to prosecute these claims in a continuation application.

SECTION 103 REJECTION OF CLAIMS 18 AND 21

As best understood, the Office concedes *Thomson*'s failure to disclose encrypting any of the data in its tables. The Office proposes to overcome this deficiency in the teaching of *Thomson* by combining with it *Denning*'s disclosure of encrypting selected fields in a database.

Proposed modification would change principle of operation

Applicant submits that the proposed modification is improper because

> *"[i]f the proposed modification...would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious."*[1]

To show why the proposed modification changes the principle of operation, consider what might happen if one were to encrypt data in some of the cells associated with "DEPT 020"

---

[1] *MPEP* 2143.01, referring to *In re Ratti*, 270 F.2d 810 (CCPA 1959).

(see *Thomson*, FIG. 4). According to the teaching of *Thomson*, the user "11111" has access to all data associated with "DEPT 020," including, of course, the encrypted data. Naturally, the user would somehow have to acquire a key for decrypting the encrypted data.

There is no discussion in *Thomson* of how the user might acquire such a key. This is not surprising since, as the Office concedes, *Thomson* fails to disclose encrypting any data. A reference that never mentions encryption can hardly be expected to describe where a key might be hidden. Any discussion of how the user might actually acquire the key would therefore have to be found in *Denning*.

In *Denning,* only a single "trusted interface" has access to the database.[2] All encryption and decryption is carried out by this trusted interface, which alone knows the key.[3] Thus, according to *Denning*, every time a user wants to decrypt data, he must call upon the trusted interface to carry out the decryption. Consequently, the trusted interface is apt to become a bottleneck to data access as the number of users increases.

In contrast, the users in *Thomson* directly access data[4] using conventional software.[5] This avoids burdening *Thomson*'s central server (which would be analogous to *Denning*'s "trusted interface") with requests to decrypt data.

It is apparent that any modification of *Thomson* to accommodate the system of *Denning* would fundamentally change this principle by which *Thomson* operates. Such a modification would replace *Thomson*'s idea of allowing users to individually access data with a formula that is virtually guaranteed to increase latency of data access.

---

[2] *Denning*, page 243 ("Because the database system may have security holes, all access to the database system is confined to a trusted (verified) interface.").
[3] *Denning*, page 243 ("the secret key *K* is known only to the trusted interface, and all encryption and decryption is done in the interface").
[4] *Thomson*, col. 6, lines 15-17 ("The relational database software contained in the server computer **12** is conventionally configured to allow direct user read access solely to the various views and the security table TABLE-S.").
[5] *Thomson*, col. 6, lines 29-33 ("Various electronic spreadsheet software and/or report generation software is typically used in the various remote terminals **14** to actually access and manipulate the various databases").

No motivation to combine the references

Applicant draws attention to the requirement that references can only be combined "when there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art."[6]

The Office has proposed, as a motivation for combining the references, that the resultant database would be "more secure." The Office has not indicated where in the cited references this motivation is found. Nor has the Office provided any chain of objective reasoning that would suggest the proposed combination.

Applicant submits that the proposed motivation of "enhancing security" is overly simplistic. After all, one can just as easily enhance security by locking the database in a room and throwing away the key. The Office's proposed motivation naively overlooks a principal challenge of database design, namely that of providing security *and* rapid access at the same time.

Because of its lack of support by any cited art or any objective reasoning, it appears that the proposed motivation may have been inadvertently contrived in hindsight using Applicant's own disclosure as a template. Applicant requests that the Office consider this possibility in connection with the withdrawal of the section 103 rejection.

Claim 56 includes limitations similar to claim 18. Accordingly, claim 56 is patentable for at least the reasons discussed above in connection with claim 18.

Claims dependent on claims 18 and 56 all contain the limitations of their respective parent claims, and are allowable for at least the same reasons.

For reasons set forth above, Applicant requests reconsideration and withdrawal of the section 103 rejection of claims 18 and 56, and all claims dependent thereon.

---

[6] *MPEP 2143.01*, referring to *In re Fine*, 937 F.2d 1071 (Fed. Cir. 1998) and *In re Jones*, 958 F.2d 347 (Fed. Cir. 1992).

SECTION 103 REJECTION OF CLAIMS 41, 48, 79, AND 86

Applicant re-asserts the arguments made in connection with claim 18 concerning the impropriety of combining the references. As discussed therein, the proposed combination of references is improper both because the result would change the principle of operation of *Thomson*, and because the motivation to combine the references appears to be contrived in hindsight to reconstruct the claimed invention.

The proposed combination of *Denning* and *Thomson*, even if it were somehow to be considered proper, fails to teach claim 41's limitation of "storing the first and second *cryptographic information* outside the table." The proposed combination also fails to teach the limitation of "information stored outside the table" that includes "*cryptographic information*," as recited in claims 48 and 86, and claim 79's limitation of "storing the first and second *cryptographic information* apart from the two columns of data."

Thomson discloses storing, outside a database, information indicative of which users may see which data. *Denning* teaches storing labels, such as "top secret," outside the database. Neither of these amounts to storing "cryptographic information." There is nothing "cryptographic" about labeling data "top secret." *Denning*'s idea of labeling data "top secret" is no different from stamping the words "top secret" on a document. The placement of such a label does nothing to *encrypt* the document.

For similar reasons, there is nothing "cryptographic" about *Thomson*'s security table, with its listing of which users may see which data. To list all those with permission read a document, as *Thomson* teaches, does not amount to *encrypting* anything. One who lacked such permission could still read the document if he could somehow obtain it. After all, the document itself is not encrypted.

Thus, even if one were to combine the cited references, the result would still fail to teach every limitation of the foregoing claims. Accordingly, the section 103 rejection of those claims is improper.

Claims dependent on the foregoing independent claims all recite the limitations of their respective parent claims, and are allowable for at least the same reasons.

For reasons set forth above, Applicant requests reconsideration and withdrawal of the section 103 rejection of claims 41, 48, 79, 86, and all claims dependent thereon.

SECTION 103 REJECTION OF CLAIMS 32, 44, 51, 69, 82, 89

These claims all depend on independent claims that have been discussed above. As such, all the arguments made in connection with the proposed combination of *Denning* and *Thomson* also apply to these claims. What follows are remarks concerning the additional reference, *Abraham*.

The Office concedes that even when combined, *Denning* and *Thomson* still fail to disclose encrypting information for providing access. To supply this missing disclosure, the Office draws attention to *Abraham* col. 7, lines 42-50, which discloses that one can store encrypted keys in a variety of locations.

To establish a prima facie case of obviousness, there must be both

- a reasonable expectation of success,[7] and
- a suggestion or motivation, either in the references or in knowledge generally available, to combine the references.[8]

Abraham discloses that one might store an encrypted key on any of a variety of storage media, for example, a disk. The Office appears to be suggesting that this knowledge, when provided to one of ordinary skill, would suggest the idea of storing the encrypted key in the security table shown in *Thomson*'s FIG. 4. Applicant suggests that in fact, one of ordinary skill would reject any such idea because it would have no reasonable expectation of success.

---

[7] *In re Merck*, 800 F.2d 1091 (Fed. Cir. 1986); *MPEP* 2143.02
[8] *MPEP* 2142, referring to (*In re Vaeck*, 947 F.2d 488 (Fed. Cir. 1991).

The table in FIG. 4 of *Thomson* lacks a suitable place to actually store this encrypted key. One could hardly store it in the first column of the table, since that column lists the users. Nor could one store it in any subsequent column, since those columns identify data that particular users can see. For this reason alone, the proposed idea of storing any key, whether encrypted or not, in the security table would immediately be dismissed as being impractical.

Suppose, however, that this difficulty could somehow be overcome and that somehow, a user could obtain, from the security table, an encrypted version of a key to unlock the desired data. For reasons that will become apparent, let us call this key the "inner" key.

Since the inner key is encrypted, the user would have to decrypt it before using it. Where then would the user obtain an "outer" key needed to decrypt this encrypted "inner" key? Would the outer key also be stored in the security table? If so, then it is either stored in clear text, or it is stored encrypted. If the former were true, then it is unclear what the point of encrypting the inner key would have been, since the outer key is so readily available. This approach would be just like writing a message in a secret code and then giving away the key. If the latter were true, then there would have to be yet another key, a "further-outer" key, to decrypt the outer key. This would again raise the question of where to store this "further-outer" key.

The Office's proposal to combine the teaching of *Abraham* with that of *Denning* and *Thomson* plainly results in a system that does not work. The only apparent motivation for combining these references appears to be that of reconstructing Applicant's claimed invention in hindsight.

The proposed combination of references is also improper because there is no suggestion to combine the references.

Both *Denning* and *Thomson* relate to database management systems. *Abraham*, however, is directed to providing secure communication between a smart card and a workstation. There is no discussion in *Abraham* of database management systems, in which many users compete to

access the same data. Hence, it is unclear how *Abraham* could even be pertinent to the technical problem addressed by *Denning* and *Thomson*.

Neither *Thomson* or *Denning* suggests that a key would be maintained separately from the database. It is unclear then why one reading *Thomson* and *Denning*, neither of which even mentions storing keys separately from the database, would suddenly be motivated to consider storing those keys in encrypted form.

Applicant submits therefore that the section 103 rejection of the foregoing claims is improper both because: (1) the proposed combination yields a system with no reasonable expectation of success; and (2) because there is no suggestion to combine *Abraham* with *Thomson* and *Denning*. Applicant also maintains that the section 103 rejection is improper for the reasons discussed in connection with claim 18.

SUMMARY

Now pending in this application are claims 18-54 and 56-92, of which claims 18, 41, 48, 56, 74, and 86 are independent. Enclosed is a $1020 check for the Petition for Extension of Time fee. Also enclosed is payment of $300 for six additional dependent claims offset by two cancelled claims. No additional fees are believed to be due in connection with this filing of this response However, to the extent fees are due, or if a refund is forthcoming, please adjust our deposit account 06-1050 referring to Attorney Docket No. "17299-008002."

Respectfully submitted,

Date: May 16, 2005

Faustino A. Lichauco
Reg. No. 41,942

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906
21041116.doc